

Code optimization, frozen glassy phase and improved decoding algorithms for low-density parity-check codes

Haiping Huang

*Department of Computational Intelligence and Systems Science,
Tokyo Institute of Technology, Yokohama 226-8502, Japan*

(Dated: September 19, 2014)

The statistical physics properties of low-density parity-check codes for the binary symmetric channel are investigated as a spin glass problem with multi-spin interactions and quenched random fields by the cavity method. By evaluating the entropy function at the Nishimori temperature, we find that irregular constructions with heterogeneous degree distribution of check (bit) nodes have higher decoding thresholds compared to regular counterparts with homogeneous degree distribution. We also show that the instability of the mean-field calculation takes place only after the entropy crisis, suggesting the presence of a frozen glassy phase at low temperatures. When no prior knowledge of channel noise is assumed (searching for the ground state), we find that a reinforced strategy on normal belief propagation will boost the decoding threshold to a higher value than the normal belief propagation. This value is close to the dynamical transition where all local search heuristics fail to identify the true message (codeword or the ferromagnetic state). After the dynamical transition, the number of metastable states with larger energy density (than the ferromagnetic state) becomes exponentially numerous. When the noise level of the transmission channel approaches the static transition point, there starts to exist exponentially numerous codewords sharing the identical ferromagnetic energy.

PACS numbers: 89.90.+n, 02.70.-c, 89.70.-a, 75.10.Nr

I. INTRODUCTION

In modern wireless communication, reliable transmission of information in a noisy environment can be achieved, proved by Shannon who put forward the celebrated channel encoding theorem [1, 2]. This theorem states that the error-free transmission is possible as long as the code rate R (the ratio between the number of bits in the original message and the number of bits in the transmitted message) does not exceed the capacity of the channel (Shannon's bound). The relation between spin glass models and information theory was first well established by Sourlas in 1989 [3]. After that, statistical physics methods especially replica trick was applied to analyze the typical properties of coding and decoding problems [4–12], and the dynamical properties of decoding process [13]. Studies of this line over decades have achieved significant results, some of which are not able to be easily obtained using traditional methods of information theory, and all these results are remarkably consistent with those of information theory [14].

The channel encoding theorem does not tell us how to construct an optimal code that saturates the Shannon's bound. Information theory community have devoted lots of efforts to devise (near) optimal codes over last several decades [15]. Codes of Gallager type are promising candidates since they have vanishing bit error rate and can saturate the Shannon limit. Gallager type error correcting code (also known as low-density parity-check (LDPC) code) was first discovered in 1962 [16], but was abandoned soon due to the limited computational ability at that time. This code was rediscovered by Mackay and Neal in 1996 [17]. Since then, the LDPC codes were extensively studied in either construction schemes or decoding algorithms. Methods of statistical physics, complementary to those used in information theory, enable one to attain a complete picture of decoding process by analyzing global properties of the corresponding free energy landscape. They also allow one to optimize the performances of various codes by changing some construction parameters. Additionally, the coding and decoding process can be mapped onto the factor graph [18] (also called Tanner graph [14]) with locally tree-like structure, which facilitates the statistical mechanics analysis.

The known picture for Gallager-type codes is [7, 13]: for sufficiently small noise levels in a transmission channel, the ferromagnetic solution is the only stable solution and the complete decoding is possible. Simple local search algorithm can recover the corrupted bits. However, as the noise level increases up to the spinodal or dynamical transition point where an exponentially large number of metastable states appear (these states are suboptimal ferromagnetic solutions and hide the original message), decoding algorithms finally fail to identify the solution in available time scales. Recent studies using one step replica symmetry breaking theory showed that the theoretical decoding limit can be pushed to a higher value [9]. This implies that in this computationally hard region [19], detailed study of codeword space structure and even metastable state landscape is needed, which might suggest novel efficient decoding schemes and insights towards the glassy dynamics of local search heuristics. When the noise level crosses the thermodynamic (static) transition point, a fraction of the metastable states are degenerate with the true codeword, and error-free

communication becomes impossible. This transition point is upper-bounded by the Shannon limit.

In this paper, we provide several physical insights for understanding the LDPC codes. First, by tuning the construction parameter, we compute the *entropy* value at the Nishimori temperature [20] (equivalently we have the prior knowledge of the channel statistics, e.g., the noise level), which reveals that the irregular constructions where degree of nodes in the factor graph follows a distribution are able to tolerate higher noise levels for reliable transmission, compared with the regular counterparts with fixed degree of nodes in the factor graph.

Second, to probe the geometrical structure of codewords, we also compute the free energy as a function of temperatures. It is found that the *entropy crisis* (the free energy takes a maximal value at a finite temperature) occurs before the instability of the mean-field calculation, which shows the existence of a frozen glassy phase at low temperatures [7, 21]. At zero temperature, the decoding process amounts to searching for the ground state. In this situation, in the presence of high enough noise level, long-range correlation develops and the first-level assumption (replica symmetric approximation) breaks down, consequently, one has to adopt replica symmetry breaking scenario as a better approximation, under which the complexity of metastable states (growth rate of the number of metastable states with the system size) is computed, implying that the number of metastable states with higher energy starts to grow exponentially when the dynamical transition is approached. When the noise level of the channel exceeds the critical point, even the number of states sharing the same energy with the unique true ferromagnetic state, starts to proliferate exponentially.

Finally, we observe divergence of local fields in the glassy regime, consistent with the frozen picture of codeword space structure. Furthermore, we show that a reinforced belief propagation (rBP) can *improve* the decoding performance at zero temperature, although the same scheme has little effects on optimal decoding (at Nishimori temperature). The associated decoding threshold almost coincides with the dynamical transition predicted by the theory. The frozen codeword picture explains the algorithmic hardness for the improved algorithm [35].

The rest of this paper is organized as follows. The low-density parity-check code and the associated spin glass model are introduced in Sec. II. In Sec. III, we compute typical value of the free energy function by using the cavity method [18], and derive the mean-field formulae for the entropy function at the Nishimori temperature, under the replica symmetric (RS) ansatz. Furthermore, we derive the one-step replica symmetry broken (1RSB) solution for the current problem when RS ansatz becomes incorrect at zero temperature. In this section, we also present a reinforced belief propagation algorithm for improving zero temperature decoding performance on single instances. In Sec. IV, the numerical simulation results on single instances and the theoretical prediction of RS and 1RSB approximations are obtained and discussed. We give final remarks and summary in Sec. V. Details of the numerical method to solve 1RSB equations in Sec. IIIB are collected in Appendix A.

II. MODEL

The information transmission process in modern wireless communication can be formulated as a channel coding problem [1, 14], in which a message of length N is transformed into a redundant transmitted message of length $M(> N)$. The encoded message is called codeword. We assume each entry of the message takes Boolean value 0, 1. The original message is denoted by $\boldsymbol{\xi}$, while the transmitted message by \mathbf{t} . The encoding process is completed by taking $\mathbf{t} = \mathbf{G}^T \boldsymbol{\xi}$ [15, 16], where $\mathbf{G} = [\mathbf{I} | (\mathbf{C}_2^{-1} \mathbf{C}_1)^T]$, i.e., a concatenation of two matrixes. \mathbf{I} is an $N \times N$ identity matrix. \mathbf{G} is chosen such that $\mathbf{H} \mathbf{G}^T = 0$ with the parity-check matrix $\mathbf{H} = [\mathbf{C}_1 | \mathbf{C}_2]$. \mathbf{C}_1 and \mathbf{C}_2 are $(M - N) \times N$ and $(M - N) \times (M - N)$ sparse matrixes respectively. Upon encoding, the message \mathbf{t} is transmitted through a noisy channel which we assume binary symmetric and memoryless, i.e., the channel is characterized by the following probability:

$$p_n(\zeta_i) = (1 - p)\delta(\zeta_i) + p\delta(\zeta_i - 1), \quad (1)$$

where the noise level p is the flip rate of the channel. The received message is corrupted by the noise as $\mathbf{r} = \mathbf{t} + \boldsymbol{\zeta}$, in which each bit is flipped independently by the noise. The symmetry property of the channel means that the conditional probability $P(r_i = 0 | t_i = 0) = P(r_i = 1 | t_i = 1) = 1 - p$, and $P(r_i = 0 | t_i = 1) = P(r_i = 1 | t_i = 0) = p$. For the binary symmetric channel (BSC), the Shannon bound is expressed as $R_c = 1 - H_2(p)$ where $H_2(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$ is the binary entropy. The decoding is carried out by calculating the so-called syndrome vector \mathbf{z} [14]:

$$\mathbf{z} = \mathbf{H} \mathbf{r} = \mathbf{H} \boldsymbol{\zeta}. \quad (2)$$

An estimate of the original message $\boldsymbol{\xi}$ is then obtained as the first N bits of $\mathbf{r} + \mathbf{n}$, where \mathbf{n} is the estimate of the true noise vector $\boldsymbol{\zeta}$, obtained by solving the parity check equations [22]:

$$\mathbf{z} = \mathbf{H} \mathbf{n}. \quad (3)$$

All the above matrix computation is based on mod 2 addition. To define our mean-field model, we transformed the Boolean variable n_i into the Ising one σ_i via $\sigma_i = (-1)^{n_i}$, and thus the mod 2 addition corresponds to a product. In the remaining part, the noise ζ_i becomes an Ising variable as well.

Introducing an inverse temperature β as a control parameter, the posterior probability of a spin configuration $\boldsymbol{\sigma}$ is given by the Bayes theorem [23]:

$$P(\boldsymbol{\sigma}|\mathbf{z}) = \frac{\exp(-\beta\mathcal{H}(\boldsymbol{\sigma}))}{Z}, \quad (4)$$

where Z is the partition function depending on the channel statistics and code constructions. The Hamiltonian is then defined as

$$\mathcal{H}(\boldsymbol{\sigma}) = -\gamma \sum_{\mu=1}^{M-N} \left(\prod_{i \in \partial\mu} \sigma_i - 1 \right) - F \sum_{i=1}^M \zeta_i \sigma_i, \quad (5)$$

where $\partial\mu$ denotes the neighbors of check μ , and a gauge transformation $\sigma_i \rightarrow \sigma_i \zeta_i$ has been made [24], which leads to the presence of random fields in the last term. The magnitude of the random field is obtained from the priori probability of the noise as $F = \frac{1}{2} \ln \frac{1-p}{p}$. γ will be finally sent to infinity to enforce $M - N$ parity-check constraints in Eq. (3). $\partial\mu$ denotes the set of non-zero entries in μ -th row of the parity check matrix \mathbf{H} . Note that the above code construction implies that \mathbf{H} is an $(M - N) \times M$ sparse matrix, whose total number of non-zero entries in each row k and that in each column l follow the degree profile (\mathcal{P}, Λ) where $\Lambda(x) = \sum_l \Lambda_l x^l$ and $\mathcal{P}(x) = \sum_k \mathcal{P}_k x^k$. In this context, we define the mean field model on a random factor graph in which the mean node (bit) degree $\langle l \rangle = \Lambda'(1)$ and the mean function node (check) degree $\langle k \rangle = \mathcal{P}'(1)$ [25]. As shown in fig. 1, the factor graph is a bipartite graph on which there are two kinds of nodes: one is the variable node (bit) and the other is the function node (check). An edge joins a variable node i and a function node μ if and only if the bit i is involved in μ -th parity check equation. We can also deduce the edge-perspective degree [18] profile $(\lambda_l = l\Lambda_l / \langle l \rangle, \rho_k = k\mathcal{P}_k / \langle k \rangle)$, specifying the probabilities that a randomly selected edge is connected to a node of degree l and to a function node of degree k , respectively. The regular code is defined when only one Λ_l (Λ_k) is non-zero, then the code rate can be obtained by $R = N/M = 1 - l/k$, where l and k are replaced by their mean value for irregular codes [26].

III. MEAN-FIELD COMPUTATION

To study the free-energy landscape of error-correcting codes, we define the following partition function:

$$Z = \sum_{\boldsymbol{\sigma}} e^{-\beta\mathcal{H}(\boldsymbol{\sigma})} \quad (6)$$

where $\mathcal{H}(\boldsymbol{\sigma})$ is defined in Eq. (5). In the thermodynamic limit, the entropy density s can be computed via:

$$s = \frac{1}{M} \ln Z - \frac{\beta F}{M} \sum_i \zeta_i m_i. \quad (7)$$

The free energy density $f \equiv -T \ln Z/M$ and the magnetization $m_i \equiv \langle \sigma_i \rangle_{P(\boldsymbol{\sigma}|\mathbf{z})}$ will be calculated under the mean field approximation in the following sections.

A. Replica symmetric approximation

We first derive the formula under the replica symmetric approximation [12, 18]. The key idea is that, in a modified graph where a bit node i is removed, then all the incoming probabilities $\hat{p}_{\mu \rightarrow i}(\sigma_i)$ become independent with each other, which is reasonable when the graph is sparse and the glass transition does not happen (there are no long-range correlations on the graph). $\hat{p}_{\mu \rightarrow i}(\sigma_i)$ denotes the probability that a check constraint μ is satisfied given the value of σ_i . Thus one can write down the free energy contribution of a bit node (see fig. 1):

$$e^{-\beta\Delta f_i} = \sum_{\sigma_i} e^{\beta h_i \sigma_i} \prod_{\mu \in \partial i} \hat{p}_{\mu \rightarrow i}(\sigma_i), \quad (8)$$

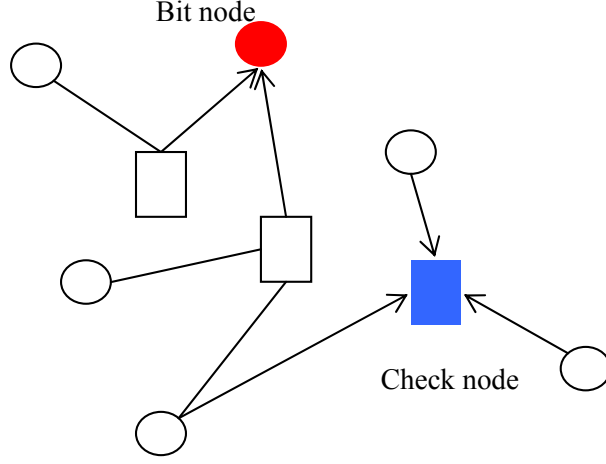


FIG. 1: (Color online) Factor graph representation of LDPC codes. The graph consists of two kinds of nodes (bit node and check node). The arrow shows the passing messages (cavity probabilities) to compute the free energy contribution of adding one bit node or one check node (the full nodes).

where ∂i denotes the neighbors of bit i , and the external field $h_i = F\zeta_i$. Likewise, in a modified graph where a function node μ is removed, then all the incoming probabilities $p_{i \rightarrow \mu}(\sigma_i)$ are also independent with each other. $p_{i \rightarrow \mu}(\sigma_i)$ denotes the probability that bit i takes value σ_i in the absence of check μ . Thus the free energy contribution of a function node (see fig. 1) can be expressed as:

$$e^{-\beta \Delta f_\mu} = \sum_{\{\sigma_i\}: i \in \partial \mu} \delta_{\prod_{i \in \partial \mu} \sigma_i, 1} \prod_{i \in \partial \mu} p_{i \rightarrow \mu}(\sigma_i), \quad (9)$$

where δ -function ensures that the parity check constraint μ is satisfied. Interested readers can find details about Eqs. (8) and (9) in Ref. [12] for the cavity method applied to error correcting codes. Finally, one can parameterize these two probabilities as $p_{i \rightarrow \mu}(\sigma_i) = \frac{1+m_{i \rightarrow \mu} \sigma_i}{2}$ and $\hat{p}_{\mu \rightarrow i}(\sigma_i) = \frac{1+\hat{m}_{\mu \rightarrow i} \sigma_i}{2}$, and get the free energy density

$$f = \frac{1}{M} \sum_i \Delta f_i - \frac{1}{M} \sum_\mu (k_\mu - 1) \Delta f_\mu, \quad (10)$$

where k_μ is the degree of function node μ and the last term avoids the double counting arising in the first term. The free energy density is clearly a function of parameters $\{m_{i \rightarrow \mu}, \hat{m}_{\mu \rightarrow i}\}$, whose values should make the free energy density stationary. In other words, the recursive equations for $m_{i \rightarrow \mu}, \hat{m}_{\mu \rightarrow i}$ can be derived from a variational principle [27]. The result is summarized as follows:

$$m_{i \rightarrow \mu} = \frac{e^{\beta h_i} \prod_{\nu \in \partial i \setminus \mu} [1 + \hat{m}_{\nu \rightarrow i}] - e^{-\beta h_i} \prod_{\nu \in \partial i \setminus \mu} [1 - \hat{m}_{\nu \rightarrow i}]}{e^{\beta h_i} \prod_{\nu \in \partial i \setminus \mu} [1 + \hat{m}_{\nu \rightarrow i}] + e^{-\beta h_i} \prod_{\nu \in \partial i \setminus \mu} [1 - \hat{m}_{\nu \rightarrow i}]}, \quad (11a)$$

$$\hat{m}_{\mu \rightarrow i} = \prod_{j \in \partial \mu \setminus i} m_{j \rightarrow \mu}, \quad (11b)$$

where $\partial \mu \setminus i$ denotes the neighbors of check μ with i excluded, while $\partial i \setminus \mu$ denotes the neighbors of bit i with μ excluded. Once the iteration of Eq. (11) reaches a fixed point, the free energy contributions Δf_i and Δf_μ can be computed as:

$$-\beta \Delta f_i = \ln \left[e^{\beta h_i} \prod_{\mu \in \partial i} \frac{1 + \hat{m}_{\mu \rightarrow i}}{2} + e^{-\beta h_i} \prod_{\mu \in \partial i} \frac{1 - \hat{m}_{\mu \rightarrow i}}{2} \right], \quad (12a)$$

$$-\beta \Delta f_\mu = \ln \left[\frac{1 + \prod_{i \in \partial \mu} m_{i \rightarrow \mu}}{2} \right]. \quad (12b)$$

The magnetization m_i in Eq. (7) can be computed using Eq. (11a) with μ included. The above formulae can be applied on single instances.

To study the typical property (e.g. computing typical entropy value) of the problem, one should carry out the average over the quenched disorder (channel statistics Eq. (1) and code constructions). The free energy density is then given by

$$f = \sum_l \Lambda_l \langle \Delta f_i \rangle_{\text{pop}} - \frac{\langle l \rangle}{\langle k \rangle} \sum_k \mathcal{P}_k(k-1) \langle \Delta f_\mu \rangle_{\text{pop}}, \quad (13)$$

where the subscript pop means that the quantity is computed from a population dynamics procedure. In practice, one starts from an initial population of $\{m_{i \rightarrow \mu}\}$ of size \mathcal{N} , whose elements are updated according to Eq. (11) until a stationary population is reached. The average is then carried out using this stationary population which is detected if the free energy density yields small fluctuation across iterations. Note that the edge-perspective degree distribution should be used when the incoming magnetizations $\{m_{j \rightarrow \mu}\}$ (or conjugated magnetizations $\{\hat{m}_{\nu \rightarrow i}\}$) are sampled in Eq. (11).

The decoding performance can be evaluated by the decoding overlap:

$$\rho = \frac{1}{M} \left\langle \sum_i \zeta_i \text{sgn} \langle \sigma_i \rangle_\beta \right\rangle = \int dm \phi(m) \text{sgn}(m), \quad (14)$$

where the gauge transformation has been performed and the inner average is the thermal average, while the outer average is the disorder one. $\phi(m) = \sum_l \Lambda_l \int \prod_{\nu=1}^l P_\nu(\hat{m}_\nu) \langle \delta(m - \mathcal{F}(\{\hat{m}_\nu\})) \rangle$ where P_ν represents the distribution of incoming conjugated magnetization in the population dynamics, and the average is taken with respect to the channel statistics. $\mathcal{F}(\cdot)$ is given by the right hand side of Eq. (11a) including contributions from all neighbors of a bit node.

B. Zero temperature decoding: 1RSB computation

The stability of iterations of Eq. (11) depends on the temperature and the noise level, which can be checked by adding a small perturbation to the cavity magnetization on each edge, and then updating the cavity magnetization and this additional variance [28], denoted by $v_{i \rightarrow \mu}$ whose evolution follows $v_{i \rightarrow \mu} = \sum_{\nu \in \partial i \setminus \mu} \sum_{j \in \partial \nu \setminus i} \left(\frac{\partial m_{i \rightarrow \mu}}{\partial m_{j \rightarrow \nu}} \right)^2 v_{j \rightarrow \nu}$. If the total strength of the variances on all edges grows with the iteration, the decorrelation assumption to derive Eq. (11) breaks down, implying that long-range correlation sets in among all nodes on the graph. This does happen in the presence of low enough temperature and high enough noise level. Therefore, we should consider one-step replica symmetry breaking assumption when $T = 0$, which concentrates the Gibbs measure defined in Eq. (4) on the ground state configurations.

Under 1RSB ansatz, the state space splits into an exponential number of macroscopic states. Each state has its own free energy density f_α with α being the state index. The Gibbs measure correspondingly decomposes into contributions of various free energy densities [29], which is described by introducing a generalized free energy function $\Phi(y)$:

$$e^{M\Phi(y)} = \sum_\alpha e^{-yMf_\alpha} = \int d\epsilon e^{M(\Sigma(\epsilon) - y\epsilon)}, \quad (15)$$

where the complexity $\Sigma(\epsilon)$ is the growth rate function of the number of states with the code length (system size) M [30]. The inverse-temperature-like parameter y is used to fix the free energy density (energy density ϵ in the zero temperature limit) of state, similar to the fact that the temperature is used to select the energy of configurations. Using definition Eq. (15), one can derive the generalized free energy contribution of a bit node i ($\Delta\Phi_i = \ln \langle e^{-y\Delta f_i} \rangle$) and that of a function node μ ($\Delta\Phi_\mu = \ln \langle e^{-y\Delta f_\mu} \rangle$), where the average is taken under 1RSB approximation. Note that in Eq. (15), we have taken the zero temperature limit while keeping a finite value of y [13]. We denote $m_{i \rightarrow \mu} \equiv \tanh \beta h_{i \rightarrow \mu}$ and $\hat{m}_{\mu \rightarrow i} \equiv \tanh \beta u_{\mu \rightarrow i}$. The free energy contributions Δf_i and Δf_μ are obtained from Eq. (12) in the limit $\beta \rightarrow \infty$:

$$\Delta f_i = - \left| h_i + \sum_{\mu \in \partial i} u_{\mu \rightarrow i} \right| + \sum_{\mu \in \partial i} |u_{\mu \rightarrow i}|, \quad (16a)$$

$$\Delta f_\mu = 2\Theta \left(- \prod_{j \in \partial \mu} h_{j \rightarrow \mu} \right) \min(|h_{j \rightarrow \mu}|, j \in \partial \mu), \quad (16b)$$

where $\Theta(x)$ is a step function taking values $\Theta(x) = 0$ for $x \leq 0$, $\Theta(x) = 1$ for $x > 0$. The distribution of $\{h_{i \rightarrow \mu}, u_{\mu \rightarrow i}\}$ satisfies the following 1RSB equation [30]:

$$P(h_{i \rightarrow \mu}) \propto \int \left[\prod_{\nu \in \partial i \setminus \mu} du_{\nu \rightarrow i} Q(u_{\nu \rightarrow i}) \right] e^{-y \Delta f_{i \rightarrow \mu}} \delta(h_{i \rightarrow \mu} - \mathcal{F}_h(\{u_{\nu \rightarrow i}\})), \quad (17a)$$

$$Q(u_{\mu \rightarrow i}) = \int \left[\prod_{j \in \partial \mu \setminus i} dh_{j \rightarrow \mu} P(h_{j \rightarrow \mu}) \right] \delta(u_{\mu \rightarrow i} - \mathcal{F}_u(\{h_{j \rightarrow \mu}\})), \quad (17b)$$

where \mathcal{F}_h and \mathcal{F}_u represent the zero temperature limit of Eq. (11) and the explicit form is given in Sec. III C. The reweighting factor $e^{-y \Delta f_{i \rightarrow \mu}}$ takes into account the reshuffling of free energies of different states when an edge $i \rightarrow \mu$ is removed [31]. This factor intuitively discourages (large) positive free energy change due to this cavity operation. The 1RSB equation (17) can be solved through a population dynamics procedure [27]. We give the details of the algorithm in Appendix A. During the iteration of Eq. (17), one can also calculate the generalized free energy and other thermodynamic quantities such as complexity, free energy. These quantities of interest can be computed by the following Legendre transformation [13]:

$$\Phi(y) = \sum_l \Lambda_l \langle \Delta \Phi_i \rangle - \frac{\langle l \rangle}{\langle k \rangle} \sum_k \mathcal{P}_k(k-1) \langle \Delta \Phi_\mu \rangle, \quad (18a)$$

$$\Sigma(\epsilon) = \Phi(y) + y\epsilon, \quad (18b)$$

$$\epsilon = -\frac{\partial \Phi(y)}{\partial y}. \quad (18c)$$

When the number of iteration is sufficiently large, the stationary value of the above thermodynamic quantities can be obtained by the bootstrap method [32].

We finally remark that Eq. (17) could not be further simplified to an efficient survey propagation algorithm [18], mainly due to the fact that the support of the cavity field distribution is not a finite discrete set, and consequently a time-consuming sampling is required even in application to single instances [33]. Furthermore, the finite value of y should also be optimized.

C. Reinforced belief propagation

In this section, we give the belief propagation equations in the limit of $\beta \rightarrow \infty$. Taking $\beta \rightarrow \infty$ in Eq. (11) leads to the following recursive equation (recall that $m_{i \rightarrow \mu} \equiv \tanh \beta h_{i \rightarrow \mu}$ and $\hat{m}_{\mu \rightarrow i} \equiv \tanh \beta u_{\mu \rightarrow i}$):

$$h_{i \rightarrow \mu} = h_i + \sum_{\nu \in \partial i \setminus \mu} u_{\nu \rightarrow i}, \quad (19a)$$

$$u_{\mu \rightarrow i} = \text{sgn} \left(\prod_{j \in \partial \mu \setminus i} h_{j \rightarrow \mu} \right) \min(|h_{j \rightarrow \mu}|, j \in \partial \mu \setminus i), \quad (19b)$$

where $\text{sgn}(x) = x/|x|$ for $x \neq 0$ and $\text{sgn}(0) = 0$. One can apply the above iteration on single instances to infer the true noise vector ζ , as $\sigma_i = \text{sgn}(H_i)$ in which $H_i = h_i + \sum_{\mu \in \partial i} u_{\mu \rightarrow i}$ and $\{u_{\mu \rightarrow i}\}$ should be the stationary value. However, in the glassy phase, the iteration fails to converge or converges to a suboptimal solution ($\rho < 1$). To circumvent this problem, one can alternatively use the reinforcement strategy [34–36]. In this situation, the external field is not constant but keeps being updated as $h_i \rightarrow h_i + \text{sgn}(H_i)\delta$ at each step with probability $1 - t^{-r}$, where t is the iteration step and r is the updating rate. At each step, one can also check if the decoding overlap equals to unity (perfect recovery of the original message). With a properly chosen value of (δ, r) , the iteration would converge to the true noise vector within certain maximal number of iterations. The optimal values for δ and r can be obtained from several trials of decoding experiments. Note that in each experiment, both parameters take values of small magnitude. We will present the numerical simulation results at $T = 0$ in Sec. IV C.

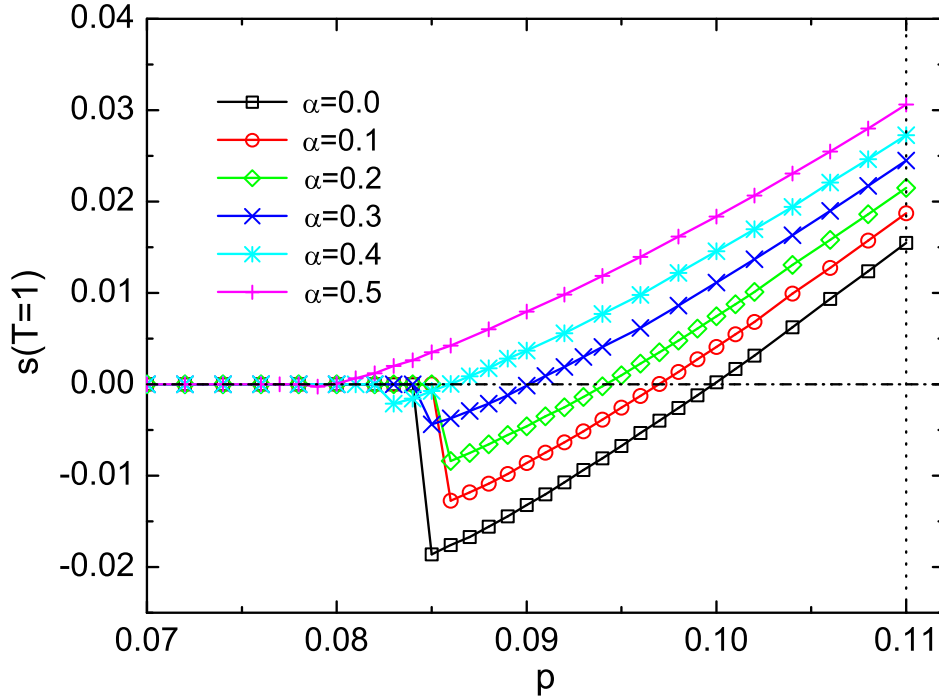


FIG. 2: (Color online) Entropy density as a function of noise level p for different code constructions (code rate $R = 0.5$). The temperature $T = 1$. The vertical dotted line shows the Shannon's bound $p_s(R = 0.5) \simeq 0.110028$.

IV. RESULTS AND DISCUSSIONS

In this section, we first present computation of entropy at the Nishimori temperature $\beta = 1$. $\beta = 1$ corresponds to the correct knowledge of the channel statistics characterized by the noise level p . At this special temperature, the RS approximation is correct and no further step replica symmetry breaking is needed [7, 20]. Decoding at $T = 1$ gives the best performance among all temperatures [20]. In real situation, we do not know the true noise level of the noisy channel. Then we can find alternatively the ground state configuration during the decoding process, which entails the 1RSB analysis. The statistical mechanical analysis of zero temperature decoding is presented in the third and fourth parts of this section. Irregular and regular codes are both analyzed, in other words, we assume $(\Lambda_2, \Lambda_3) = (\alpha, 1 - \alpha)$, $(\mathcal{P}_4, \mathcal{P}_6) = (\alpha, 1 - \alpha)$ and other coefficients vanish, such that the defined code ensemble has code rate $R = 0.5$. $\alpha = 0$ corresponds to the regular code under consideration.

A. Entropy at the Nishimori temperature

The entropy density at the Nishimori temperature is shown in fig. 2. At the low noise level, there exists a ferromagnetic state whose entropy vanishes and the decoding overlap is always unity. The energy of the ferromagnetic state can be computed as $f_{\text{ferro}} = -(1 - 2p)F$ by setting $s = 0$, and $m_i = 1 \ \forall i$ [7]. As the noise level increases up to a point where the entropy function starts to become negative, metastable states with higher energy appear and compete with the dominant ferromagnetic state. The normal belief propagation would thus get stuck in one of these suboptimal metastable states. In this sense, this transition point is called the dynamical transition, denoted by p_d . The negativity of the entropy is due to the emergence of metastable states, whose behavior as a function of the energy density can be computed under 1RSB ansatz and will be shown later. Note that in this region, replica symmetry is still correct for thermodynamically dominant state [37]. When the noise level reaches a point called static (thermodynamic) transition point p_c , the entropy continuously becomes positive, implying that the number of codewords degenerate with the true one proliferates exponentially. Beyond the static transition, reliable decoding is impossible, since multiple codewords dominate the state space and one can not identify which one is the correct codeword. p_c evaluated at the Nishimori temperature coincides with that of zero temperature decoding [38], which was already shown by assuming a frozen glassy phase [7].

From fig. 2, one can also deduce that the irregular code ensemble has a larger p_d , but increasing α makes the

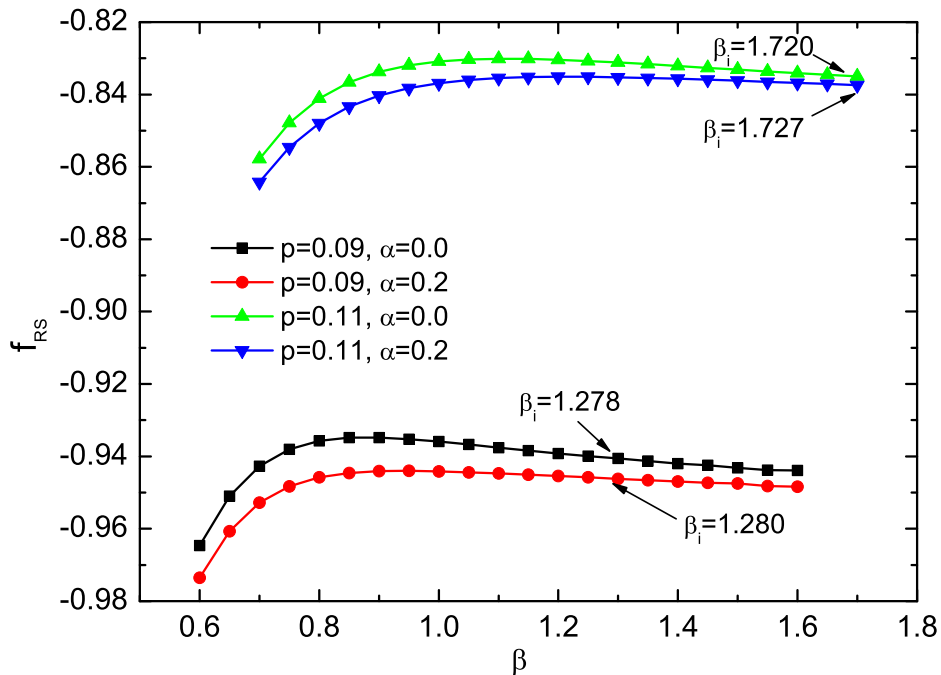


FIG. 3: (Color online) Free energy density as a function of inverse temperature for regular ($\alpha = 0.0$) and irregular ($\alpha = 0.2$) codes. The curve develops a maximal value at a finite temperature β_s^{-1} where the entropy ($s = \beta^2 \partial f_{RS} / \partial \beta$) vanishes. Furthermore, the temperature where the RS ansatz becomes unstable is always lower than β_s^{-1} . For the curve from the top to the bottom, the instability temperature β_i is 1.720, 1.727, 1.278, 1.280 respectively.

separation between p_d and p_c smaller and smaller. It seems that the irregular code with $\alpha = 0.2$ has the largest p_d of all α shown in the figure. The superior performance of irregular codes has also been found in similar contexts [13, 25, 26, 39], but here we focus on the channel of BSC, which is different from the case of binary erasure channel for which analytical results can be derived [13]. A recent study found that for a chain of multiple locally-coupled LDPC ensembles, p_d of the coupled system approaches p_c of the original ensemble, which is called threshold saturation via spatial coupling [40].

B. The entropy crisis

In fig. 3, we show the free energy as a function of inverse temperature. A maximum develops at a finite temperature defined as β_s^{-1} . The stability analysis in Sec. IIIB shows that β_s is always smaller than the instability inverse temperature β_i , suggesting that a discontinuous phase transition must appear at $\beta_c \leq \beta_s$ [21] and a frozen glassy phase is present. When calculating the complexity function, we find that the updating local fields in Eq. (17) tend to diverge for larger values of y , consistent with the frozen picture. The frozen glassy phase implies that 1RSB states are reduced to isolated configurations with zero internal entropy, which is a direct result of the hard constraints in Eq. (5) (the first term). Similar phenomenon was also observed in the binary perceptron problem [41] and other hard constraint satisfaction problems [21]. For the decoding problem at the zero temperature, the frozen picture is related to the difficulty for local search heuristics to find the true sent message, since a rearrangement of many bits is needed when changing one bit to satisfy all parity-check constraints.

C. Zero temperature decoding: improvement by reinforced belief propagation

In this section, we first show the typical property of zero temperature decoding, and then show an improvement of decoding performance by applying reinforced belief propagation on single instances. In fig. 4 (a), we show the comparison between the calculated free energy (Eqs. (13) and (16)) and the ferromagnetic one. Before p_d , these two free energies coincide, implying that the ferromagnetic state is the unique dominant state without suboptimal metastable states. At p_d , the calculated free energy jumps to a higher value, and keeps decreasing as p further

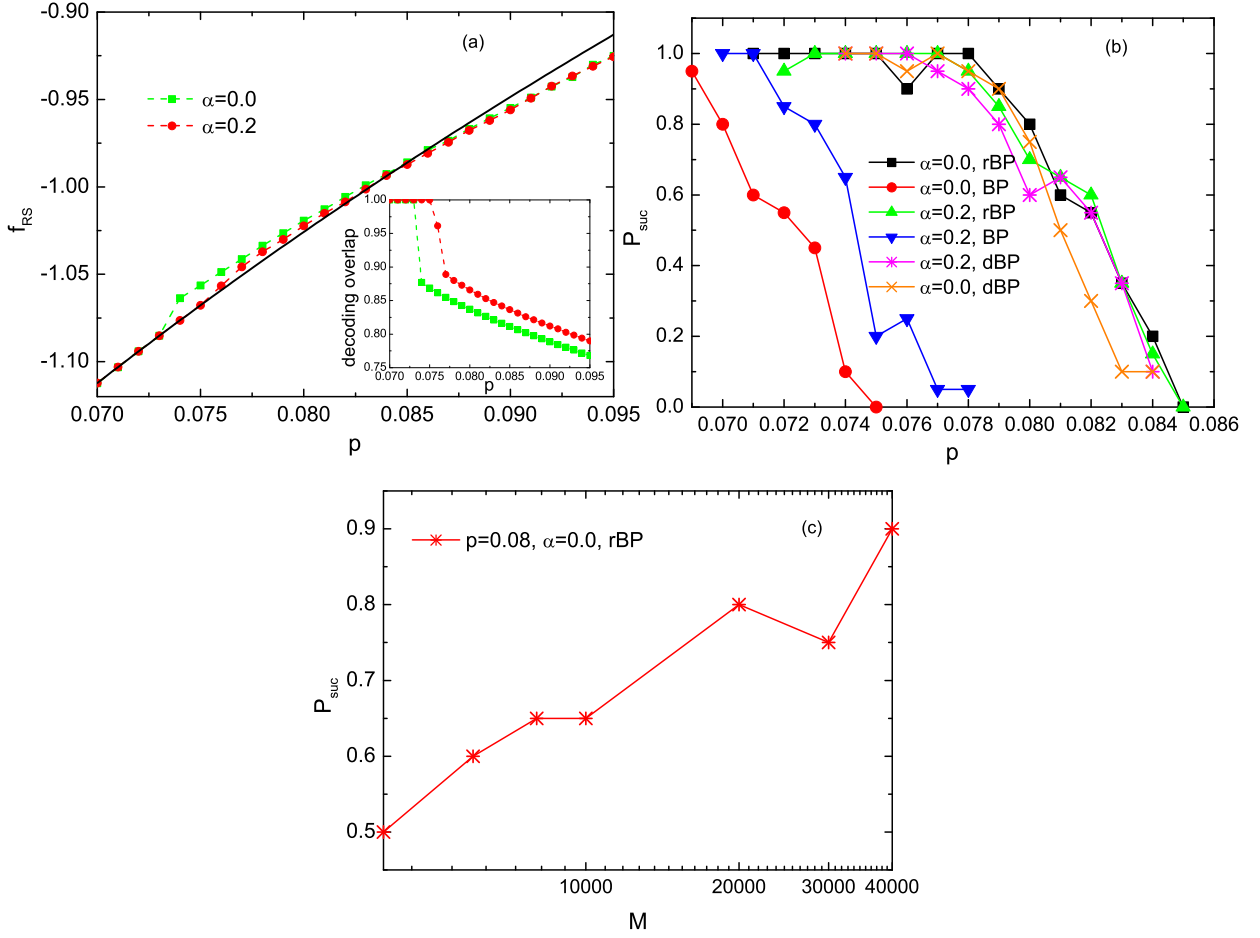


FIG. 4: (Color online) (a) Phase transition for the zero temperature decoding. The full line represents the free energy of ferromagnetic state. The inset shows the transition in terms of decoding overlap. (b) Probability of successful decoding as a function of noise level. Performances of rBP, BP and dBP are compared. Code length $M = 20000$. Code rate $R = 0.5$ and the probability is computed over 20 random samples. $(r, \delta) = (0.04, 0.01)$ for rBP. The maximal number of iterations is equal to 1500. (c) P_{succ} versus the code length M . Other parameters are the same as those in (b).

increases, until the thermodynamic transition point is reached. After the thermodynamic transition p_c , the calculated free energy becomes lower than the ferromagnetic one, signalling that a large number of codewords contribute to the Gibbs measure and as a result, the ferromagnetic one ceases to be dominant. This picture gives a rough estimate of the phase transition points [9]. More accurate determination requires further steps of replica symmetry breaking, as analyzed in Refs. [9, 13]. In the inset of fig. 4 (a), we see clearly that the irregular code has higher decoding threshold than the regular one, even when the decoding is performed at the zero temperature.

Zero temperature decoding aims at finding the ground state configuration as the inferred noise vector. As expected, normal belief propagation (Eq. (19)) yields the same decoding threshold as predicted in fig. 4 (a). Surprisingly, the decoding performances can be improved by applying an additional updating external field to the normal BP iterations, the so-called reinforcement strategy [34, 36]. Due to emergence of metastable states with higher energy, normal BP converges to these suboptimal states or fails to converge within a maximal number of iterations. However, the reinforcement during the iteration can bring the evolution of the passing messages (cavity fields) on the links of factor graph to the desired codeword. The decoding threshold can be pushed to a value as high as $p \simeq 0.082$ ($P_{succ} = 0.5$) [39]. This value almost coincides with the theoretical decoding limit (p_d). It should be mentioned that we also apply the same strategy to optimal temperature decoding ($T = 1$), but it has little effects on the decoding performances, i.e., yielding similar threshold with normal BP. Thus, we conclude that, when the frozen glassy phase sets in, both BP and rBP fail to recover the original message. However, by using rBP, one can succeed in decoding at noise levels where normal BP fails, as long as $p < p_d$, which is related to the fact that rBP is more robust against complex energy landscape than BP in decoding performance. The decoding performance of rBP versus the code length is also shown in fig. 4 (c). The finite size effect implies that the successful decoding is achieved with high

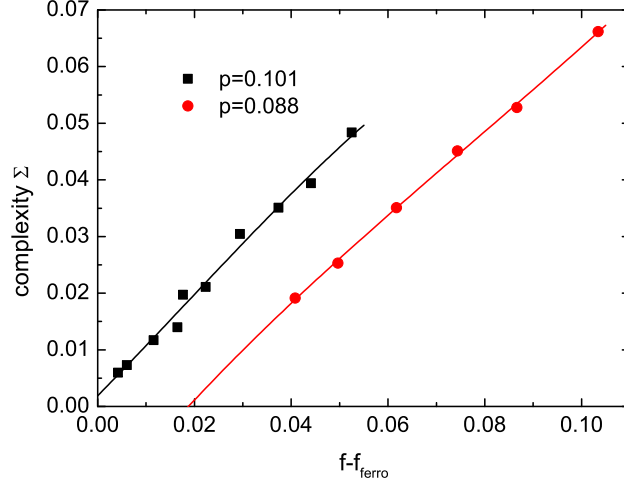


FIG. 5: (Color online) Complexity as a function of free energy difference $f - f_{\text{ferro}}$ for a regular code system ($\alpha = 0$). Only the physical concave part of the curve is shown. $p = 0.101 \simeq p_c$ and $p = 0.088 > p_d \simeq 0.084$. Curves are polynomial fits of degree 3.

probability for long-length codes as long as the noise level is below the threshold.

Finally, we remark that, by damping the updated message, i.e., $h_{i \rightarrow \mu}^{t+1} = \kappa h_{i \rightarrow \mu}^{t+1} + (1 - \kappa) h_{i \rightarrow \mu}^t$ (dBP), where κ is a small damping factor taking 0.05 in our simulations, one can also improve the decoding performance of BP yielding comparable results with those of rBP (see fig. 4 (b)). However, the convergence of rBP to the true ferromagnetic state is typically fast, e.g., rBP takes a median of 241 iteration steps, while dBP takes a median of 364 iteration steps for decoding the regular code of length $M = 20000$ at $p = 0.08$. Although dBP performs slightly worse than rBP particularly around the decoding threshold, they both improve greatly over the normal BP. This is mainly due to the fact that, during the iteration, their newly updated messages memorize the old messages at the preceding step in different manners, suggesting that a memory of the history of updating messages plays an important role in improving the decoding performance especially when the complex energy landscape is present.

D. Zero temperature decoding: typical free-energy landscape under 1RSB ansatz

In this section, we study the typical property of free energy landscape of zero temperature decoding under 1RSB ansatz, by solving the 1RSB equations derived in Sec. III B. Only the regular code with $\alpha = 0$ is considered, and qualitative behavior is expected for irregular codes. We consider the complexity as a function of the free energy difference $f - f_{\text{ferro}}$. The result is reported in fig. 5. The population dynamics details to solve the 1RSB equations (Eq. (17)) are presented in Appendix A. Varying the inverse-temperature-like parameter y from zero to positive value, we first observe a convex unphysical part, followed by a concave physical part which is shown in fig. 5 for $p = 0.088$ and $p = 0.101$. When p is larger than p_d but below p_c , the complexity at certain $f > f_{\text{ferro}}$ becomes positive, demonstrating that the unique dominant state is the ferromagnetic one, whereas, numerous high-lying metastable states are present, as shown in the plot. These high-lying metastable states hide the true ferromagnetic state, making the local search heuristics (such as simulated annealing or normal BP) is difficult to find the desired noise vector of the channel [13]. p_d is thus defined as the point where a non-trivial concave part of the complexity curve starts to appear. When the noise level becomes larger than p_c , even at ferromagnetic free energy, the complexity has a positive value, suggesting that the metastable states have the same energy with the ferromagnetic state which is not the unique one any more. Therefore decoding is impossible in general due to the fact the number of valid codewords grows exponentially with the code length. p_c is thus defined as the point where the complexity at f_{ferro} starts to be positive.

V. SUMMARY

In this work, we provide a detailed statistical mechanics analysis of low-density parity-check codes. The computation of entropy value at the Nishimori temperature shows that one can improve the decoding performance (shift the theoretical decoding threshold to a higher value) by adopting the irregular code with optimal construction parameters.

The free energy function at different temperatures shows that an entropy crisis occurs before the instability of RS computation, which establishes the discontinuous nature of the phase transition located at a temperature larger than or equal to the entropy crisis temperature. Hard nature of the parity-check constraints provides an intuitive understanding of the frozen picture of codeword space structure. The divergence of cavity fields observed in solving 1RSB equations also supports this important feature of LDPC codes.

At zero temperature, we find that the decoding performance can be improved by applying a reinforced strategy during the iteration of normal BP. Interestingly, this strategy has little effects on temperature $T = 1$ decoding which is expected to be optimal decoding but the prior knowledge about the channel is required. The normal BP typically does not converge at high noise levels, indicating 1RSB approximation should be adopted to derive correct physical picture. Under this ansatz, one can determine the dynamical transition and thermodynamic transition by evaluating the complexity function. Above the dynamical transition but below the thermodynamic transition, the complexity becomes positive at certain higher level of energy. For the higher noise level located above the static transition point, the exponential growth of the number of degenerate codeword is observed. Our studies provide a detailed quantitative analysis of LDPC codes, in terms of code optimization, frozen glassy phase and improved decoding algorithms when no prior knowledge of channel statistics is assumed, under both RS and 1RSB approximations, and are expected to shed light on statistical mechanics analysis of other state-of-the-art error correcting codes.

Acknowledgments

This work was partially supported by the JSPS Fellowship for Foreign Researchers (Grant No. 24 · 02049). Helpful discussions with Yoshiyuki Kabashima are acknowledged.

Appendix A: Population dynamics procedure solving 1RSB equations

In 1RSB assumption, there exists a distribution of cavity fields on each edge of a general factor graph, capturing the fluctuation of cavity fields across different macroscopic states. To take into account the graph ensembles (average over different code constructions), we need a population of cavity fields with $\mathcal{N} \times \mathcal{M}$ elements, i.e., \mathcal{N} subpopulations (each of them has size \mathcal{M}). The RS case corresponds to $\mathcal{M} = 1$, and we use $\mathcal{N} = 20000$. A single update of one subpopulation proceeds in the following five steps:

1. Sample a degree of a node i from λ_l , then for each neighbor μ , sample its degree from ρ_k , finally select at random and uniformly $k - 1$ different subpopulations representing distributions on its adjacent incoming edges $j \rightarrow \mu$ except $i \rightarrow \mu$. A total number $(l - 1)(k - 1)$ of subpopulations are selected. Set an initial weight $w_0 = e^{-y\Delta f_{i \rightarrow \nu}^0}$.
2. Compute one element $h_{i \rightarrow \nu}$ using these selected subpopulations according to Eq. (17a), and calculate the cavity free energy $\Delta f_{i \rightarrow \nu}$ at the same time. This newly computed element is accepted if the new weight $w = e^{-y\Delta f_{i \rightarrow \nu}} > w_0$, otherwise the old value is retained with a probability $1 - w/w_0$.
3. Repeat (2) for each element of the subpopulation on edge $i \rightarrow \nu$ totally \mathcal{L} times (we call \mathcal{L} the sampling interval).
4. Sample a degree of a node i from Λ_l , then for each neighbor μ , sample its degree from ρ_k , finally select at random and uniformly $k - 1$ different subpopulations representing distributions on its adjacent incoming edges $j \rightarrow \mu$ except $i \rightarrow \mu$. A total number $(k - 1)l$ of subpopulations are selected. Using these subpopulations, one can compute $\langle \Delta \Phi_i \rangle$ by repeating totally $\mathcal{L}\mathcal{M}$ sampling procedures.
5. Sample a degree of a function node μ from \mathcal{P}_k and repeat step (1) to (4) k times to get k new subpopulations, which can be used to evaluate $\langle \Delta \Phi_\mu \rangle$ using $\mathcal{L}\mathcal{M}$ samples.

In practice, the above procedure is iterated for \mathcal{T} steps (in unit of \mathcal{N}) with the first \mathcal{T}_0 steps discarded. The generalized free energy in Eq. (18a) can be obtained from the data of the later $\mathcal{T} - \mathcal{T}_0$ iterations. In fact, the reweighting process is carried out by using the Metropolis importance-sampling method [42]. Other techniques can be found in the book [18]. The parameters for the above population dynamics procedure are $(\mathcal{N}, \mathcal{M}, \mathcal{L}) = (1024, 1024, 70)$ and $(\mathcal{T}, \mathcal{T}_0) = (400, 200)$. Effects of \mathcal{L} on the complexity function are summarized in fig. 6, which shows that a sufficiently large \mathcal{L} should be chosen to ensure the reliable evaluation of relevant thermodynamic quantities.

[1] C. E. Shannon, Bell System Tech. J **27**, 379 (1948).

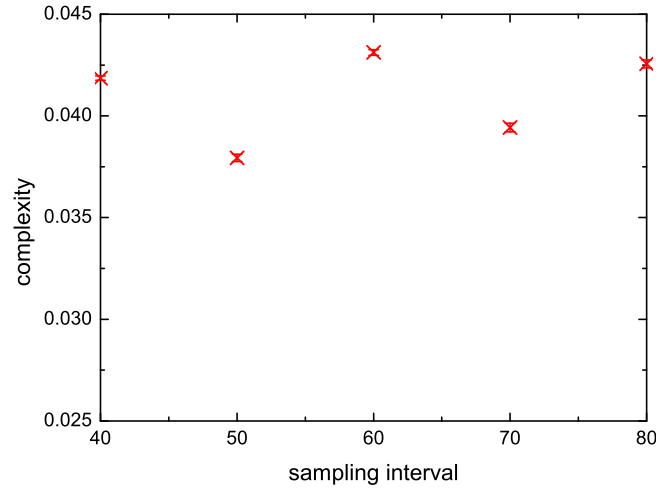


FIG. 6: (Color online) Complexity as a function of sampling interval for a regular code system ($\alpha = 0$). $y = 0.82$ for $p = 0.101$.

- [2] C. E. Shannon, Bell System Tech. J **27**, 623 (1948).
- [3] N. Sourlas, Nature **339**, 693 (1989).
- [4] H. Nishimori and K. Y. M. Wong, Phys. Rev. E **60**, 132 (1999).
- [5] I. Kanter and D. Saad, Phys. Rev. Lett **83**, 2660 (1999).
- [6] Y. Kabashima, T. Murayama, and D. Saad, Phys. Rev. Lett **84**, 1355 (2000).
- [7] A. Montanari, Eur. Phys. J. B **23**, 121 (2001).
- [8] T. Tanaka and D. Saad, J. Phys. A **36**, 11143 (2003).
- [9] G. Migliorini and D. Saad, Phys. Rev. E **73**, 026122 (2006).
- [10] T. Mora and O. Rivoire, Phys. Rev. E **74**, 056110 (2006).
- [11] I. Neri, N. S. Skantzos, and D. Bolle, J. Stat. Mech p. P10018 (2008).
- [12] H. Huang and H. Zhou, Phys. Rev. E **80**, 056113 (2009).
- [13] S. Franz, M. Leone, A. Montanari, and F. Ricci-Tersenghi, Phys. Rev. E **66**, 046120 (2002).
- [14] T. Richardson and R. Urbanke, *Modern Coding Theory* (Cambridge University Press, Cambridge, 2008).
- [15] D. J. C. Mackay, IEEE Trans. Inf. Theory **45**, 399 (1999).
- [16] R. G. Gallager, IRE Trans. Inf. Theory **IT-8**, 21 (1962).
- [17] D. J. C. MacKay and R. Neal, Electronics Letters **32**, 1645 (1996).
- [18] M. Mézard and A. Montanari, *Information, physics, and computation* (Oxford University Press, Oxford, 2009).
- [19] E. Berlekamp, R. McEliece, and H. C. A. Van Tilborg, IEEE Trans. Inf. Theory **24**, 384 (1978).
- [20] H. Nishimori, J. Phys. Soc. Jpn **62**, 2973 (1993).
- [21] O. C. Martin, M. Mézard, and O. Rivoire, Journal of Statistical Mechanics: Theory and Experiment p. P09006 (2005).
- [22] Y. Kabashima, K. Nakamura, and J. van Mourik, Phys. Rev. E **66**, 036125 (2002).
- [23] Y. Kabashima and D. Saad, J. Phys. A **37**, R1 (2004).
- [24] T. Murayama, D. Saad, Y. Kabashima, and R. Vicente, Phys. Rev. E **62**, 1577 (2000).
- [25] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, IEEE Trans. Inf. Theory **47**, 619 (2001).
- [26] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, IEEE Trans. Inf. Theory **47**, 585 (2001).
- [27] M. Mézard and G. Parisi, Eur. Phys. J. B **20**, 217 (2001).
- [28] E. Marinari and G. Semerjian, Journal of Statistical Mechanics: Theory and Experiment p. P06019 (2006).
- [29] R. Monasson, Phys. Rev. Lett **75**, 2847 (1995).
- [30] M. Mézard and G. Parisi, J. Stat. Phys **111**, 1 (2003).
- [31] D. Battaglia, M. Kolar, and R. Zecchina, Phys. Rev. E **70**, 036107 (2004).
- [32] A. K. Hartmann, *A Practical Guide To Computer Simulation* (World Scientific, Singapore, 2009).
- [33] B. Wemmenhove and H. J. Kappen, J. Phys. A **39**, 1265 (2006).
- [34] A. Braunstein, F. Kayhan, G. Montorsi, and R. Zecchina, In: IEEE International Symposium on Information Theory (ISIT07) p. 1891 (2007), arXiv: 0705.0423.
- [35] L. Dall'Asta, A. Ramezani, and R. Zecchina, Phys. Rev. E **77**, 031118 (2008).
- [36] A. Braunstein, F. Kayhan, and R. Zecchina, Phys. Rev. E **84**, 051111 (2011).
- [37] M. Yoshida, T. Uezu, T. Tanaka, and M. Okada, J. Phys. Soc. Jpn **76**, 054003 (2007).
- [38] J. van Mourik, D. Saad, and Y. Kabashima, Phys. Rev. E **66**, 026705 (2002).
- [39] R. Vicente, D. Saad, and Y. Kabashima, J. Phys. A **33**, 6527 (2000).
- [40] S. Kudekar, T. Richardson, and R. Urbanke, IEEE Trans. Inf. Theory **59**, 7761 (2013).
- [41] H. Huang, K. Y. M. Wong, and Y. Kabashima, J. Phys. A **46**, 375002 (2013).
- [42] H. Zhou, Phys. Rev. E **77**, 066102 (2008).